

Scott A. Kamber
KamberLaw, LLC
100 Wall St., 23rd Fl., New York, NY 10005
Bus: 646-964-9600
Fax: 212-202-6364
Email: skamber@kamberlaw.com

Rahul Ravipudi
Panish Shea & Boyle, LLP
11111 Santa Monica Blvd, Ste. 700, Los Angeles, CA 90025
Bus: 310-477-1700
Fax: 310-477-1699
Email: ravipudi@psblaw.com

Lane K. Bennett
Law Offices of Lane K. Bennett
322 2nd Ave W.
Kalispell, MT 59903
Tel: 406-752-7300
Fax: 406-752-7300
Email: lkbennett@montanasky.us

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MONTANA
BILLINGS DIVISION**

**NEEL DEERING, individually, and
on behalf of himself and all others
similarly situated,**

Plaintiffs,

v.

**CENTURYTEL INC., *et al.*
Defendants.**

Cause No. CV-10-63-BLG-RFC

**PLAINTIFF'S PRELIMINARY
PRETRIAL STATEMENT**

Pursuant to the Court's June 15, 2010, Order and Local Rule 16.2(b)(1), Plaintiff Neil Deering hereby provides the Court with his Preliminary Pretrial Statement.

A. Brief Factual Outline.

In late 2007, for a period extending until late June, the Defendant, CenturyTel Broadband Services, LLC ("CenturyTel"), an Internet Service Provider, diverted substantially all of the Internet communications of its customers in and around Kalispell, Montana, as well as other communities in Montana, Wyoming, and Idaho, to an Internet ad-serving company called NebuAd, Inc. ("NebuAd"). CenturyTel accomplished this by installing, within its Internet network, a device provided by NebuAd. CenturyTel positioned the NebuAd device "inline," physically connecting it so all Internet communications to and from its customers flowed unfiltered through the device. These intercepted communications were then routed to and from NebuAd, again via the device. NebuAd reviewed *all* of the intercepted information and profiled CenturyTel's affected customers. Based on these profiles, NebuAd served advertisements to CenturyTel's customers which were intended to be more "relevant" to them. However, as part of NebuAd's operations under its contract with CenturyTel, NebuAd tampered with Internet communications being sent back to customers in order to escape detection by security tools on customers' personal computers. CenturyTel has admitted in Congressional testimony that these activities were not in its regular course of business as an ISP, nor were they necessary to protect CenturyTel or its customers. Moreover, at no time did CenturyTel obtain the consent of its customers to intercept and funnel all of their actions/information to a third party.

Based on these actions, Plaintiff brought suit against CenturyTel, individually and on behalf of a class of similarly situated individuals, for violations of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2701 *et seq.*, as well as the Computer

Fraud and Abuse Act (“CFAA”), 18 § U.S.C. 1030 *et seq.*, invasion of privacy by intrusion upon seclusion, unjust enrichment and trespass to chattels.

B. Issues Concerning Jurisdiction and Venue

This Court has personal jurisdiction over Defendant because a substantial portion of the wrongdoing alleged in this complaint took place in the State of Montana and Defendant is authorized to do business in and has sufficient minimum contacts with this state and/or has otherwise intentionally availed itself of the markets in this State to render the exercise of jurisdiction by this Court permissible under traditional notions of fair play and substantial justice.

Venue is proper in this District under Title 28, United States Code, Sections 1391(b) and (c), in that Defendant conducts business with consumers in this District, and a substantial portion of the events and conduct giving rise to the violations of law set forth *infra* took place in this District.

C. Factual Basis of Each Claim

At this time, Plaintiffs allege the following claims:

1. Defendant indiscriminately intercepted and inspected all of its customers’ Internet communication. Defendant identified and monitored not just individual accounts, but individual users. Defendant tampered with communications received by users to insert advertisements and avoid detection. Defendant tampered with users’ personal computers for tracking purposes, causing non-standard cookies to be created on users’ personal computers, and which users could not manage using standard privacy management tools.

2. Defendant intentionally intercepted Plaintiff’s electronic communications and used the contents of said communications knowing and having reason to know that the

information was obtained through unlawful interception. Plaintiff's electronic communications were in fact intercepted and intentionally used.

3. Defendant intentionally accessed computers without authorization and exceeded authorized access and thereby obtained confidential information. Defendant knowingly caused the transmission of programs, information, codes, or commands, and as a result intentionally and recklessly caused damage to protected computers. Such damage resulted in an aggregated loss of at least \$5,000 within a one-year period to each group of Plaintiffs affected by each appliance.

4. Defendant, without authority or consent, interfered with and intermeddled with Plaintiffs' personal computers and Internet communications. Defendant's conduct harmed Plaintiffs' personal property and diminished its value, quality, condition, and utility, causing real and substantial damage to Plaintiffs.

D. Legal Theory Underlying Each Claim

At this time, Plaintiffs raise the following legal theories underlying its known claims:

1. Invasion of Privacy by Intrusion Upon Seclusion: Defendant's interception and inspection, identification and monitoring of individual Users, and tampering with Users' communications and personal computers constituted tortious invasion of privacy by intrusion upon the solitude and seclusion of Users' private affairs that would be highly offensive and objectionable to a reasonable person.

2. Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2510: Defendant's conduct was in violation of Title 18, United States Code, Section 2511(1)(a) because Defendant intentionally intercepted Plaintiff's electronic communications. Defendants conduct was in violation of Section 2511(1)(d) in that Defendant used the contents of said

communications knowing and having reason to know that the information was obtained through interception in violation of Section 2511(1).

3. Violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030: Defendant, by intentionally accessing computers without authorization, acted in violation of Title 18, United States Code, Section 1030(a)(2)(A). Defendant's conduct was in violation of Section 1030(a)(5)(A) in that Defendant intentionally and recklessly caused damage through the transmission of programs, information, codes, or commands. Defendant recklessly caused damage in an aggregated loss of at least \$5,000, and thereby violated Section 1030(a)(5)(B). Lastly, Defendant's conduct was in violation of Section 1030(a)(5)(C) in that Defendant intentionally accessed protected computers without authorization, and as a result caused damage and loss.

4. Trespass to Chattels: The common law prohibits the intentional intermeddling with personal property, including a computer in another's possession, which results in the deprivation of the use of the personal property or impairment of the condition, quality, or usefulness of the property. Defendant's acts constituted repeated and persistent trespass on Plaintiffs' use and enjoyment of their computers and communications, in violation of common law.

E. Computation of Damages

ECPA provides that any person whose communications are intercepted may bring a federal, civil lawsuit against the wiretapper. 18 U.S.C. § 2520(a). Liable defendants must pay actual damages to the victims or statutory damages of \$100 per victim per day or \$10,000 per victim, whichever is greater. 18 U.S.C. § 2520(c).

At least 20,000 customers were subjected to monitoring by NebuAd's appliance, for a period of at least 180 days. Thus, CenturyTel is liable to each customer whose communications were intercepted for damages in the amount of \$18,000. If the number of affected customers is indeed 20,000, CenturyTel's total statutory liability, applying the first measure of damages, is \$360,000,000. As the statute requires that victims be paid the greater of the two measures (\$10,000, as opposed to \$9,000), CenturyTel's liability is actually \$400 million.

Additionally, the CFAA provides that any person whose computer is accessed without authorization and suffers damage thereby may maintain a civil action against the violator and obtain compensatory damages. 18 U.S.C.A. § 1030(g). Accordingly, CenturyTel is liable to each customer whose computer was accessed for compensatory damages as well.

F. Pendency of Related State or Federal Litigation

The following cases are pending in this and other jurisdictions:

Valentine v. NebuAd, Inc., CV-08-5113 (N.D. Cal.).
Mortensen v. Bresnan Communications LLC, No. CV-10-13 (D. Mont.).
Valentine v. Wideopen West Finance LLC, No. 09-CV-7653 (N.D. Ill.).
Green v. Cable One, Inc., No. 10-CV-259 (N.D. Ala.).
Manard v. Knology, Inc., No. 10-CV-15 (M.D. Ga.).
Kirch v. Embarq Management Co., No. 10-CV-2047 (D. Kan.).

G. Proposed Stipulations of Fact and the Parties' Understanding as to What Law Applies

To date, the parties have not proposed stipulations of fact and law to each other.

H. Proposed Deadlines Relating to Joinder of Parties or Amendment of the Pleadings

Plaintiffs propose that any motion for leave to join additional parties or to otherwise amend the pleadings shall be filed by August 12, 2010.

I. Identification of Controlling Issues of Law Suitable for Pretrial Disposition

Plaintiffs anticipate moving for summary judgment, for the reasons set forth above.

J. Name, Address, and Telephone Number for Each Individual with Information that May Be Used in Proving or Denying Claims or Defenses, and Summary of that Information

- a. Plaintiff, in care of KamberLaw, LLC;
- b. Retained experts yet to be determined;
- c. Persons, including CenturyTel personnel, identified by CenturyTel as having knowledge;
- d. Persons whose identities are currently unknown and who were NebuAd's sales and technical support personnel interacting with CenturyTel

K. Descriptions of Documents and Data Compilations that May Be Used

- e. CenturyTel's contracts/agreements with customers affected by the deployment of the NebuAd device;
- f. CenturyTel's communications with NebuAd, including contracts, installation and operations instructions, operations reports, sales literature, correspondence, and financial transmittals;
- g. CenturyTel's internal communications regarding its relationship with NebuAd;
- h. CenturyTel's internal policies and procedures regarding operations and handling of customer communications;
- i. CenturyTel's communications with customers;
- j. CenturyTel personnel documentation regarding organization and reporting responsibilities of persons involved in engaging NebuAd and deploying NebuAd equipment and services;
- k. The physical and technical configuration document of CenturyTel's high-speed networks;
- l. CenturyTel's computer network operations change logs;
- m. All contracts and agreements between CenturyTel and any other Internet ad-serving companies, Internet ad agencies, or Internet ad exchanges, at any time;
- n. Any communications from customers regarding service levels, performance, and functioning of their personal computers during the relevant time period.

L. Insurance Agreements

Plaintiffs are unaware of applicable insurance agreements other than as disclosed by Defendant.

M. Status of Settlement Discussions and Prospects for Compromise

The parties have not conducted preliminary settlement discussions.

N. Suitability of Special Procedures

The parties have not identified any applicable special procedures.

N. Discovery Plan

The parties are finalizing and filing their joint discovery plan forthwith.

DATED this 30th day of June, 2010

Respectfully submitted,

s/Rahul Ravipudi
Rahul Ravipudi
Admitted *pro hac vice*
PANISH SHEA & BOYLE, LLP
One of the Attorneys for Plaintiff